El documento que se redacta a continuación tiene como objeto identificar y describir funciones, acciones y servicios que realiza el Equipo de Respuesta ante Emergencias Informáticas nacional (CERT.ar), en el marco de la norma RFC- 2350.

Dentro de la información que se menciona, se describe la estructura de la organización, la identificación del equipo, su composición y misión, así como también, el ámbito de actuación y los servicios prestados.

1. INFORMACIÓN DEL DOCUMENTO

1.1- Fecha de la última actualización

Versión 1.1, publicada el 20 de mayo del 2023

1.2- Lista de distribución para notificaciones

Los cambios a este documento no se distribuyen por una lista de correo. Cualquier pregunta o comentario específico, dirigirse por favor a la dirección de correo reportes@cert.ar .

2- INFORMACIÓN DE CONTACTO

2.1- Nombre del equipo

Equipo de Respuesta ante Emergencias Informáticas nacional (CERT.ar)

2. 2- Zona horaria

GMT-3 horas

2.3- Otras telecomunicaciones

No existen

2.4-Correo electrónico

reportes@cert.ar

2.5. Otra información

La información general de los servicios proporcionados por el CERT.ar se encuentra publicada en https://argentina.gob.ar/cert-ar

El CERT.ar es miembro del FIRST: https://www.first.org/members/teams/cert-ar

El CERT.ar es miembro del CSIRTAmericas: https://csirtamericas.org/es/member_teams

2.6. Puntos de contacto con el cliente

Por medio de correo electrónico a la dirección reportes@cert.ar

Horario de Atención: El equipo de respuesta a incidentes está disponible en los siguientes horarios:

- Consultas sobre servicios y reportes de incidentes: horario de oficina (9.00h-17.00h)
- Incidentes catalogados con criticidad muy alta o crítica: 24x7x365.

2.7. Claves públicas y cifrado de información

El correo electrónico de contacto puede recibir información cifrada por medio de PGP. La clave pública asociada se encuentra en el siguiente link: https://github.com/cert-ar/PGP-Key

3- CARTA

3.1-Misión

El CERT.ar fue creado el 19 febrero del 2021, mediante la Disposición Administrativa 1/2021 de la Dirección Nacional de Ciberseguridad. Su misión es coordinar la gestión de incidentes de seguridad a nivel nacional y prestar asistencia en aquellos que afecten a las entidades y jurisdicciones del Sector Público Nacional, definidas en el inciso a) del artículo 8° de la Ley Nº 24.156 y sus modificatorios, y a las Infraestructuras Críticas de Información, declaradas como tales.

En la Disposición mencionada, se describe que el CERT.ar tiene las siguientes funciones:

- Administrar y gestionar toda la información sobre reportes de incidentes de seguridad en las entidades y jurisdicciones del Sector Público Nacional definidas en el inciso a) del artículo 8° de la Ley N° 24.156 y sus modificatorios.
- Asesorar técnicamente ante incidentes de seguridad en sistemas informáticos que reporten las entidades y jurisdicciones enumeradas más arriba.
- Coordinar las acciones a seguir, ante incidentes de seguridad, con otros Programas y equipos de respuestas a incidentes de la República Argentina.
- Contribuir a incrementar la capacidad de prevención, alerta, detección y recuperación ante incidentes de seguridad informática que puedan afectar activos de información críticos del país.
- Interactuar y cooperar con equipos de similar naturaleza de otros países.
- Llevar un registro de estadística y establecer métricas a nivel nacional.
- Coordinar la gestión de incidentes de seguridad informática que afecten recursos críticos a nivel nacional.
- Coordinar la gestión de incidentes de seguridad informática que afecten recursos críticos a nivel nacional.

- Impulsar la formación de capacidades de prevención, detección, alerta y recuperación para la respuesta ante incidentes de seguridad informática.
- Cooperar con los gobiernos provinciales y de la Ciudad Autónoma de Buenos Aires en la gestión de incidentes de seguridad informática.

3.2 - Comunidad atendida

Los incidentes atendidos por el CERT.ar son aquellos que afectan a sistemas de la administración pública nacional (inciso a) del artículo 8° de la Ley Nº 24.156 y sus modificatorios y a las Infraestructuras Críticas de Información, declaradas como tales). Cumple además las funciones de CERT Coordinador a nivel Nacional.

3.3- Patrocinio y/o afiliación

El CERT.ar es el Equipo de Respuesta ante Emergencias Informáticas nacional de la Dirección Nacional de Ciberseguridad, un organismo que depende de la Subsecretaría de Tecnologías de la Información de la Secretaría de Innovación Pública, de la Jefatura de Gabinete de Ministros Argentina.

3.4. Autoridad

El objetivo principal es la coordinación de la respuesta a incidentes y el manejo adecuado que deben tener los constituyentes de los mismos.

La autoridad del CERT.ar emana de las siguientes disposiciones:

- Disposición 1/2021
- Disposición 7/2021
- Decisión Administrativa 641/2021

El CERT.ar no tiene autoridad y/o responsabilidad sobre las infraestructuras tecnológicas de su comunidad objetivo. Todas las actividades se basan en relaciones de colaboración con otras entidades responsables de infraestructuras a nivel nacional e internacional.

4-POLÍTICAS

4.1. Tipos de incidentes y nivel de soporte

Los servicios prestados por el equipo CERT.ar proporcionan asesoramiento técnico-administrativo para la resolución de incidentes de ciberseguridad.

También se ofrecen otros servicios, como pueden ser realizar test de penetración, organización de ciber-ejercicios y entrenamientos, entre otros. Estos servicios pueden ser solicitados y el equipo los prestará de acuerdo a su disponibilidad.

Los incidentes se categorizan en función de sus características haciendo uso de la taxonomía empleada por el CERT.ar, la cual se basa en la taxonomía utilizada por INCIBE para la Clasificación de Incidentes de Seguridad.

4.2. Cooperación, interacción y divulgación de información

La información manejada por el CERT.ar es tratada con absoluta confidencialidad de acuerdo a las políticas y procedimientos para la gestión de incidentes establecidos por el organismo, así como por las políticas y normas de seguridad utilizadas para la protección de la información clasificada.

De igual modo, toda la información suministrada al organismo será utilizada para ayudar a resolver incidentes de seguridad, y sólo se distribuirá a otros equipos y miembros según la necesidad específica y de forma anónima.

El CERT.ar considera muy importante la cooperación operativa y el intercambio de información entre los distintos Equipos de Respuesta a Incidentes y también con otras organizaciones nacionales e internacionales que puedan contribuir a sus servicios o hacer uso de ellos.

El CERT.ar adopta el protocolo de señalización de intercambio de información (TLP). https://www.first.org/tlp/

4.3. Comunicación y autenticación

El método de comunicación es el correo electrónico. No obstante, el equipo brinda contactos telefónicos para ser utilizados durante la asistencia del incidente.

5- SERVICIOS

La respuesta a incidentes proporciona disponibilidad 24/7 y generalmente incluye la evaluación de los informes entrantes sobre incidentes y el seguimiento de estos con otros CSIRT, ISP y sitios ("Coordinación de incidentes").

5.1 Clasificación del Incidente

- Ayudamos a realizar la clasificación de acuerdo a la taxonomía utilizada por el equipo.
- Evaluación y comparación del incidente con hechos históricos.

5.2. Coordinación de incidentes

- Facilitar el contacto con otros actores que puedan estar involucrados.
- Comunicarse con las partes interesadas.
- Brindar soporte general para la coordinación durante la resolución del incidente

5.3. Resolución de incidentes

- Brinda asesoramiento y soporte a la parte afectada para eliminar las vulnerabilidades o vectores de ataque, que causaron el incidente y brindar resiliencia y mayor protección a los sistemas afectados.
- Evaluar las acciones relacionadas a la resolución del incidente.
- Proporcionar asistencia en la interpretación de datos cuando sea necesario.

5.4. Prevención

La prevención y la preparación consisten en todas las actividades destinadas a reducir la probabilidad o el impacto de un incidente para nuestra comunidad objetivo. El Cert.ar proporciona información actual y asesoramiento sobre nuevas amenazas y ataques que pueden tener un impacto en las operaciones de la institución y busca crear conciencia y habilidades dentro de la comunidad. Además difunde información sobre vulnerabilidades de seguridad, alertas de intrusión, virus informáticos y proporciona recomendaciones para abordar su remediación a los miembros de su comunidad objetivo.

6- FORMULARIOS DE NOTIFICACIÓN DE INCIDENTES

El organismo posee en su página web https://www.argentina.gob.ar/jefatura/innovacion-publica/ssetic/direccion-nacional-ciberseguridad/cert-ar un formulario destinado al reporte público de posibles ciberataques, hallazgo de vulnerabilidades y/o posibles incidentes de ciberseguridad.

7- DESCARGOS DE RESPONSABILIDAD

El CERT.ar toma todas las precauciones al momento de preparar notificaciones e informes y no asume ninguna responsabilidad sobre el mal uso que se realice de la información contenida en este formulario.